

A second look at Shoup's lemma

Bruno Blanchet
blanchet@di.ens.fr

INRIA, École Normale Supérieure, CNRS, Paris

partly supported by ANR ProSe (decision 2010-VERS-004-01)

June 2011

Introduction

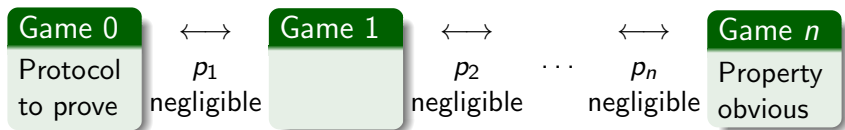
Improve **probability bounds** in proofs by sequences of games:

- **Shoup's lemma** introduces **constant factors** in probabilities of success of attacks.
 - We show that these constant factors can be eliminated.
- The **definition of secrecy** introduces a **factor 2** in the probability that an adversary breaks secrecy.
 - We show that this factor can sometimes be partly eliminated.
- Application to the password-based protocol **OEKE (One-Encryption Key Exchange)**.
 - We show that the adversary can test at most **one password per session** of the client or of the server (instead of 3 passwords per interaction with the client or server in the initial paper).
- Improvements implemented in CryptoVerif.

Proofs by sequences of games

Proofs in the computational model are typically proofs by sequences of games [Shoup, Bellare&Rogaway]:

- The first game is the **real protocol**.
- One goes from one game to the next by syntactic transformations or by applying the definition of security of a cryptographic primitive. The difference of probability between consecutive games is negligible.
- The last game is **"ideal"**: the security property is obvious from the form of the game.
(The advantage of the adversary is 0 for this game.)



CryptoVerif background: Indistinguishability

- The game G interacting with an adversary (evaluation context) C is denoted $C[G]$.
- $C[G]$ may execute events, collected in a sequence \mathcal{E} .
- A **distinguisher** D takes as input \mathcal{E} and returns **true** or **false**.
 - Example: $D_e(\mathcal{E}) = \mathbf{true}$ if and only if $e \in \mathcal{E}$. D_e is abbreviated e .
- $\Pr[C[G] : D]$ is the probability that $C[G]$ executes \mathcal{E} such that $D(\mathcal{E}) = \mathbf{true}$.

Definition (Indistinguishability)

We write $G \approx_p^V G'$ when, for all evaluation contexts C acceptable for G and G' with public variables V and all distinguishers D ,

$$|\Pr[C[G] : D] - \Pr[C[G'] : D]| \leq p(C, D).$$

Properties of indistinguishability

Lemma

- ① *Reflexivity: $G \approx_0^V G$.*
- ② *Symmetry: \approx_p^V is symmetric.*
- ③ *Transitivity: if $G \approx_p^V G'$ and $G' \approx_{p'}^V G''$, then $G \approx_{p+p'}^V G''$.*
- ④ *Application of context: if $G \approx_p^V G'$ and C is an evaluation context acceptable for G and G' with public variables V , then $C[G] \approx_{p'}^{V'} C[G']$, where $p'(C, D) = p(C'[C[]], D)$ and $V' \subseteq V \cup \text{var}(C)$.*

Shoup's lemma

Goal: bound $\Pr[C[G_0] : e_0]$.

G_0

↕ probability p

G_n

↕ $\Pr[C[G_{n+1}] : e]$

G_{n+1}

event e

↕ probability p'

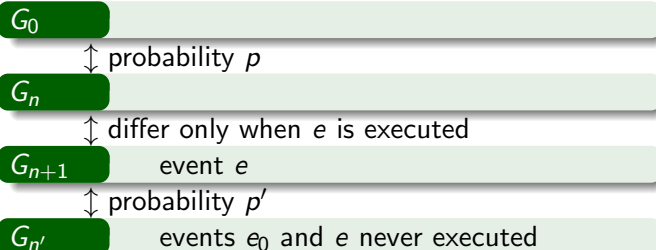
$G_{n'}$

events e_0 and e never executed

$$\begin{aligned} \Pr[C[G_0] : e_0] &\leq p + \Pr[C[G_{n+1}] : e] + p' \\ &\leq p + p' + p' \\ &\leq p + 2p' \end{aligned}$$

Improved version of Shoup's lemma

Goal: bound $\Pr[C[G_0] : e_0]$.



$$\begin{aligned}
 \Pr[C[G_0] : e_0] &\leq p + \Pr[C[G_n] : e_0] \\
 &\leq p + \Pr[C[G_{n+1}] : e_0 \vee e] \\
 &\leq p + p' + \Pr[C[G_{n'}] : e_0 \vee e] \\
 &\leq p + p'
 \end{aligned}$$

Improved Shoup's lemma

Lemma

Let C be a context acceptable for G and G' with public variables V .

① **Improved Shoup's lemma:**

If G' differs from G only when G' executes event e , then

$$\Pr[C[G] : D] \leq \Pr[C[G'] : D \vee e].$$

② If $G \approx_p^V G'$, then $\Pr[C[G] : D] \leq p(C, D) + \Pr[C[G'] : D]$.

③ $\Pr[C[G] : D \vee D'] \leq \Pr[C[G] : D] + \Pr[C[G] : D']$.

Definition of secrecy

Definition (Secrecy)

Let x be a one-dimensional array.

Let R_x be a process that

- chooses a bit b ;
- provides test queries that, on input u , return $x[u]$ when $b = 1$ and a random value $y[u]$ when $b = 0$;
- expects a value b' from the adversary and executes event S when $b' = b$.

Let C be a context acceptable for $G \mid R_x$ without public variables that does not contain S .

$$\text{Adv}_G^{\text{secrecy}(x)}(C) = 2 \Pr[C[G \mid R_x] : S] - 1$$

Definition of secrecy

Definition (Secrecy)

Let x be a one-dimensional array.

Let R_x be a process that

- chooses a bit b ;
- provides test queries that, on input u , return $x[u]$ when $b = 1$ and a random value $y[u]$ when $b = 0$;
- expects a value b' from the adversary and executes event S when $b' = b$.

Let C be a context acceptable for $G \mid R_x$ without public variables that does not contain S .

$$\text{Adv}_G^{\text{secrecy}(x)}(C) = 2 \Pr[C[G \mid R_x] : S] - 1$$

Proof of secrecy

Goal: secrecy of x in G_0

$G_0 \mid R_x$

↕ probability p

$G_n \mid R_x$

secrecy proved: $\Pr[C[G_n \mid R_x] : S] = \frac{1}{2}$

$$\begin{aligned} \text{Adv}_{G_0}^{\text{secrecy}(x)}(C) &= 2 \Pr[C[G_0 \mid R_x] : S] - 1 \\ &\leq 2(p + \Pr[C[G_n \mid R_x] : S]) - 1 \\ &\leq 2p \end{aligned}$$

Proof of secrecy with Shoup's lemma

$G_0 \mid R_x$ goal: secrecy of x in G_0

↕ probability p

$G_n \mid R_x$

↕ differ only when e is executed

$G_{n+1} \mid R_x$ event e

↕ probability p'

$G_{n'} \mid R_x$ secrecy proved: $\Pr[C[G_{n'} \mid R_x] : S] = \frac{1}{2}$

↕ probability p''

$G_{n''} \mid R_x$ event e never executed

$$\begin{aligned}
 \text{Adv}_{G_0}^{\text{secrecy}(x)}(C) &\leq 2(p + \Pr[C[G_n \mid R_x] : S]) - 1 \\
 &\leq 2(p + \Pr[C[G_{n+1} \mid R_x] : S \vee e]) - 1 \\
 &\leq 2(p + p' + \Pr[C[G_{n'} \mid R_x] : S \vee e]) - 1 \\
 &\leq 2(p + p' + \Pr[C[G_{n'} \mid R_x] : e]) \leq 2(p + p' + p'')
 \end{aligned}$$

Improved proof of secrecy with Shoup's lemma

$G_0 \mid R_x$ goal: secrecy of x in G_0

↕ probability p

$G_n \mid R_x$

↕ differ only when e is executed

$G_{n+1} \mid R_x$ event e

↕ probability p'

$G_{n'} \mid R_x$

secrecy proved: $\Pr[C[G_{n'} \mid R_x] : S] = \frac{1}{2}$

event e is independent of S

↕ probability p''

$G_{n''} \mid R_x$

event e never executed

$$\begin{aligned} \text{Adv}_{G_0}^{\text{secrecy}(x)}(C) &\leq 2(p + p' + \Pr[C[G_{n'} \mid R_x] : S \vee e]) - 1 \\ &\leq 2(p + p' + \frac{1}{2} \Pr[C[G_{n'} \mid R_x] : e]) \leq 2(p + p') + p'' \end{aligned}$$

Improved proof of secrecy with Shoup's lemma

Lemma

If CryptoVerif proves the secrecy of x in game G , and e_1, \dots, e_n are events introduced by Shoup's lemma in previous steps of the proof, then

$$\Pr[C[G \mid R_x] : S \vee e_1 \vee \dots \vee e_n] \leq \frac{1}{2} + \frac{1}{2} \Pr[C[G \mid R_x] : e_1 \vee \dots \vee e_n].$$

Events e_1, \dots, e_n are independent of S .

$$\begin{aligned} & \Pr[C[G \mid R_x] : S \vee e_1 \vee \dots \vee e_n] \\ &= \Pr[C[G \mid R_x] : S] + \Pr[C[G \mid R_x] : \neg S \wedge (e_1 \vee \dots \vee e_n)] \\ &= \frac{1}{2} + \Pr[C[G \mid R_x] : \neg S] \Pr[C[G \mid R_x] : e_1 \vee \dots \vee e_n] \\ &= \frac{1}{2} + \frac{1}{2} \Pr[C[G \mid R_x] : e_1 \vee \dots \vee e_n] \end{aligned}$$

OEKE: One-Encryption Key Exchange

OEKE [Bresson et al, CCS'03]

- The client and the server initially share a **password** pw .
- They establish a **strong key** by
 - a Diffie-Hellman key exchange
 - with one message encrypted under the password
- Assumptions:
 - Computational Diffie-Hellman assumption (CDH)
 - Ideal cipher model
 - Random oracle model

OEKE

Client U	Server S
shared pw	
$x \xleftarrow{R} [1, q - 1]$	
$X \leftarrow g^x$	$y \xleftarrow{R} [1, q - 1]$
	$Y \leftarrow g^y$
$Y \leftarrow \mathcal{D}_{pw}(Y^*)$	$Y^* \leftarrow \mathcal{E}_{pw}(Y)$
$K_U \leftarrow Y^x$	
$Auth \leftarrow \mathcal{H}_1(U S X Y K_U)$	
$sk_U \leftarrow \mathcal{H}_0(U S X Y K_U)$	$K_S \leftarrow X^y$
	if $Auth = \mathcal{H}_1(U S X Y K_S)$ then
	$sk_S \leftarrow \mathcal{H}_0(U S X Y K_S)$

Notations

- dictionary size N
- N_U client instances under active attack
- N_S server instances under active attack
- N_P sessions under passive attack
- q_h hash queries
- q_e encryption queries asked by the adversary
- $q_S \leq N_S + N_P$ server instances
- $q_{\mathcal{E}} \leq q_e + N_U + N_S + N_P$ encryption/decryption queries
- $l_1 =$ length of the output of \mathcal{H}_1
- $q =$ order of \mathbb{G}

Proof of OEKE

G_0 goal: semantic security of the key $\text{Adv}_{G_0}^{\text{ake}}(C) = 2 \Pr[C[G_0] : S] - 1$

\updownarrow probability $p_0 = \frac{q_\varepsilon^2}{2(q-1)} + \frac{q_S q_\varepsilon}{q-1} + \frac{2q_\varepsilon^2 + q_S^2}{2(q-1)}$

G_3

\updownarrow differ only when Encrypt is executed

G_4

event Encrypt

\updownarrow probability $\frac{N_S}{2^l}$

G_5

\updownarrow differ only when Auth' is executed

G_6

event Auth'

\updownarrow differ only when AskH is executed

G_7

event AskH

$\Pr[C[G_7] : S] = \frac{1}{2}$, S independent of Encrypt, Auth', and AskH

$\Pr[C[G_7] : \text{Encrypt}] \leq \frac{N_U}{N}$, $\Pr[C[G_7] : \text{Auth}'] \leq \frac{N_S}{N}$,

$\Pr[C[G_7] : \text{AskH}] \leq q_h \text{Succ}_G^{\text{cdh}}(t')$, $t' \leq t_C + (N_U + N_S + N_P + q_e + 1)\tau_G$

Standard computation of probabilities

$$\begin{aligned}
 & \Pr[C[G_0] : S] \\
 & \leq p_0 + \Pr[C[G_4] : \text{Encrypt}] + \frac{N_S}{2^{l_1}} + \Pr[C[G_6] : \text{Auth}'] + \Pr[C[G_7] : \text{AskH}] + \frac{1}{2} \\
 & \leq p_0 + 2\frac{N_S}{2^{l_1}} + 2\Pr[C[G_6] : \text{Auth}'] + 2\Pr[C[G_7] : \text{AskH}] + \frac{N_U}{N} + \frac{1}{2} \\
 & \leq p_0 + 2\frac{N_S}{2^{l_1}} + 2\left(\Pr[C[G_7] : \text{AskH}] + \frac{N_S}{N}\right) + 2\Pr[C[G_7] : \text{AskH}] + \frac{N_U}{N} + \frac{1}{2} \\
 & \leq p_0 + 2\frac{N_S}{2^{l_1}} + 4\Pr[C[G_7] : \text{AskH}] + 2\frac{N_S}{N} + \frac{N_U}{N} + \frac{1}{2} \\
 & \leq p_0 + 2\frac{N_S}{2^{l_1}} + 4q_h \text{Succ}_{\mathbb{G}}^{\text{cdh}}(t') + 2\frac{N_S}{N} + \frac{N_U}{N} + \frac{1}{2}
 \end{aligned}$$

So

$$\text{Adv}_{G_0}^{\text{ake}}(C) \leq \frac{4N_S + 2N_U}{N} + 8q_h \text{Succ}_{\mathbb{G}}^{\text{cdh}}(t') + 2p_0 + 4\frac{N_S}{2^{l_1}}$$

Improved computation of probabilities

$$\begin{aligned}
 \Pr[C[G_0] : S] &\leq p_0 + \Pr[C[G_3] : S] \\
 &\leq p_0 + \Pr[C[G_4] : S \vee \text{Encrypt}] \\
 &\leq p_0 + \frac{N_S}{2^h} + \Pr[C[G_5] : S \vee \text{Encrypt}] \\
 &\leq p_0 + \frac{N_S}{2^h} + \Pr[C[G_6] : S \vee \text{Encrypt} \vee \text{Auth}'] \\
 &\leq p_0 + \frac{N_S}{2^h} + \Pr[C[G_7] : S \vee \text{Encrypt} \vee \text{Auth}' \vee \text{AskH}] \\
 &\leq p_0 + \frac{N_S}{2^h} + \frac{1}{2} + \frac{1}{2} \Pr[C[G_7] : \text{Encrypt} \vee \text{Auth}' \vee \text{AskH}] \\
 &\leq p_0 + \frac{N_S}{2^h} + \frac{1}{2} + \frac{1}{2} \left(\frac{N_U}{N} + \frac{N_S}{N} + q_h \text{Succ}_G^{\text{cdh}}(t') \right)
 \end{aligned}$$

So

$$\text{Adv}_{G_0}^{\text{ake}}(C) \leq \frac{N_S + N_U}{N} + q_h \text{Succ}_G^{\text{cdh}}(t') + 2p_0 + 2\frac{N_S}{2^h}$$

Impact on EKE: semantic security

- Standard computation of probabilities:

$$\text{Adv}_{G_0}^{\text{ake}}(C) \leq \frac{4N_S + 2N_U}{N} + 8q_h \times \text{Succ}_G^{\text{cdh}}(t') + \text{collision terms}$$

- Improved computation of probabilities:

$$\text{Adv}_{G_0}^{\text{ake}}(C) \leq \frac{N_S + N_U}{N} + q_h \times \text{Succ}_G^{\text{cdh}}(t') + \text{collision terms}$$

- The adversary can test **one password per session** with the parties.

Impact on EKE: one-way authentication

- Standard computation of probabilities:

$$\text{Adv}_{G_0}^{\text{c-auth}}(C) \leq \frac{2N_S + N_U}{N} + 3q_h \times \text{Succ}_G^{\text{cdh}}(t') + \text{collision terms}$$

- Improved computation of probabilities:

$$\text{Adv}_{G_0}^{\text{c-auth}}(C) \leq \frac{N_S + N_U}{N} + q_h \times \text{Succ}_G^{\text{cdh}}(t') + \text{collision terms}$$

- The adversary can test **one password per session** with the parties.

Conclusion

- We **eliminate some constant factors** in probabilities, when Shoup's lemma is applied.
- (Minor) improvement in probability bounds.
- Can be important for password-based protocols, for instance.
- Applied to OEKE: **optimal bound** of one tested password per session under active attack.
- Can be applied in **manual proofs** and implemented in **CryptoVerif**.